(iii) In a mixed environment in which classified and unclassified information in processed or stored, the ''Unclassified'' label must be used to identify the media containing unclassified information. In environments in which only unclassified information is processed or stored, the use of the ''Unclassified'' label is not required. Unclassified media, however, that are on loan from (and must be returned to) vendors do not require the ''Unclassified'' label, but each requires a Data Descriptor label with the words, ''Unclassified Vendor Medium'' entered on it.

(iv) Each medium shall be appropriately affixed with a classification label and, as applicable, with a Data Descriptor label at the earliest practicable time as soon as the proper security classification or control has been established. Labels shall be conspicuously placed on media in a manner that will not adversely affect operation of the equipment in which the media is used. Once applied, the label is not to be removed. A label to identify a higher level of classification may, however, be applied on top of a lower classification level in the event that the content of the media changes, e.g., from Confidential to Secret. A lower classification label may not be applied to media already bearing a higher classification label. Personnel shall be responsible for appropriately labeling and controlling ADP and computer storage media within their possession.

(g) *Electronically Transmitted Information (Messages) [1.5(c)].* Classified information that is transmitted electronically shall be marked as follows:

(1) The highest level of classification shall appear before the first line of text;

(2) A ''CLASSIFIED BY'' line is not required;

(3) The duration of classification shall appear as follows:

(i) For information to be declassified automatically on a specific date: ''DECL: (date)'';

(ii) For information to be declassified upon occurrence of a specific event: ''DECL: (description of event)'';

(iii) For information not to be automatically declassified which requires the originating agency's determination (see also §2.7(e)(3)): ''DECL: OADR'';

(iv) For information to be automatically downgraded: ''DOWNGRADE TO (classification level to which the information is to be downgraded) ON (date or description of event on which downgrading is to occur)''.

(4) Portion marking shall be as prescribed in §2.7(a)(3);

(5) Specially designated markings as prescribed in §2.7(f) (2), (3), and (4) shall appear after the marking for the highest level of classification. These include:

(i) Restricted Data or Formerly Restricted Data;

(ii) Information concerning intelligence sources or methods: ''WNINTEL,'' unless otherwise prescribed by the Director of Central Intelligence; and

(iii) Foreign Government Information (FGI).

(6) Paper copies of electronically transmitted messages shall be marked as provided in §2.7(a) (1), (2), and (3).

(h) *Changes in Classification Markings [4.1(b)].* When a change is made in the duration of classified information, all holders of record shall be promptly notified. If practicable, holders of record shall also be notified of a change in the level of classification. Holders shall alter the markings on their copy of the information to conform to the change, citing the authority for it. If the remarking of large quantities of information is unduly burdensome, the holder may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Items withdrawn from the collection for purposes other than transfer for storage shall be marked promptly in accordance with the change notice.

§ 2.8 Limitations on classification [1.6(c)].

(a) Before reclassifying information as provided in section 1.6(c) of the Order, authorized officials, who must have original classification authority and jurisdiction over the information involved, shall consider the following factors which shall be addressed in a report to the Assistant Secretary (Management) who shall in turn forward a report to the Director of the Information Security Oversight Office:

(1) The elapsed time following disclosure;

(2) The nature and extent of disclosure;

(3) The ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed;

(4) The ability to prevent further disclosure; and

(5) The ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

(b) Information may be classified or reclassified after it has been requested under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory declassification review provisions of the Order if such classification meets the requirements of the Order and is accomplished personally and on a document-by-document basis by the Secretary of the Treasury, the Deputy Secretary, the Assistant Secretary (Management) or an official with original Top Secret classification authority. Such reclassification actions shall be reported in writing to the Departmental Director of Security.

(c) In no case may information be classified or reclassified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

Subpart B—Derivative Classification

§ 2.9 Derivative Classification Authority.

Designations of derivative classification authority for national security information are contained in Treasury Order 102–19 (or successor order). The authority to derivatively classify inheres within the office and may be exercised by a person acting in that capacity. There may be additional redelegations of derivative classification authority made pursuant to TO 102–19 (or successor order). Officials identified in Treasury Order 102–19 (or successor order) may also administratively control and decontrol sensitive but unclassified information using the legend ''Limited Official Use'' and may redelegate their authority to control and decontrol. Such redelegations shall be in writing on TD F 71–01.20 ''Designation of Controlling/Decontrolling Officials'' (or successor form).

[63 FR 14357, Mar. 25, 1998]

§ 2.10 Listing derivative classification authorities.

Delegations of derivative classification authority to officials not otherwise identified in § 2.9, shall be in writing and reported annually each October 15th to the Departmental Director of Security on TD F 71–01.18 (Report of Authorized Derivative Classifiers). Such delegations shall be limited to the minimum number absolutely required for efficient administration. Periodic reviews and evaluations of such delegations shall be made by the Departmental Director of Security to ensure that officials so designated have demonstrated a continuing need to exercise such authority. If after reviewing and evaluating the information the Departmental Director of Security determines that such officials have not demonstrated a continuing need to exercise such authority, the Departmental Director of Security shall recommend to the Assistant Secretary (Management), as warranted, the reduction or elimination of such authority. The Assistant Secretary (Management) shall take appropriate action in consultation with the affected official(s) and the Departmental Director of Security. Such action may include relinquishment of this authority where the Assistant Secretary (Management) determines that a firm basis for retention does not exist.

§ 2.11 Use of derivative classification [2.1].

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an approved classification guide.